What is the RADIUS protocol?

RADIUS is a network protocol used to authenticate and allow users to access a remote network. The term RADIUS is an acronym for Remote Authentication Dial-In User Service.

What is the RADIUS protocol? RADIUS is a network protocol used to authenticate and allow users to access a remote network. The term RADIUS is an acronym for Remote Authentication Dial-In User Service.

First introduced in 1991, RADIUS remains a powerful tool for managing network users' access. To understand why, let's take a look at the development of the RADIUS protocol over the years.

The origin of RADIUS

The origin of RADIUS
According to John Vollbrecht, founder of Interlink Networks and a key player in the advent of the RADIUS protocol, the story of RADIUS actually began in 1987 when the National Science Foundation (NSF) awarded an open contract. NSFnet extension (ie the precursor of modern Internet) to Merit Network Inc.

Merit Network Inc. is a not-for-profit corporation that has developed an exclusive network authentication protocol to connect universities across Michigan. At the time, most networks took advantage of proprietary protocols in this way. NSF's contract to expand NSFnet is an attempt to bring the Internet to the public.

However, in order to do so, Merit's proprietary network, had to be converted to NSFnet based on IP. Merit then gathered proposals from vendors to develop a protocol that could support Merit's dial-in authentication method, but for IP-based networks. They received a response from a company called Livingston Enterprises, with the proposal basically containing the description for the RADIUS protocol. Merit Networks Inc. accepted the proposal from Livingston Enterprises in 1991 and the RADIUS protocol was born.

How does RADIUS work?

RADIUS leverages the client / server model to authenticate network user access
RADIUS leverages the client / server model to authenticate network user access. In fact, require users to access the network sent from the client such as the user system or WiFi access point to the RADIUS server for authentication.

RADIUS servers are usually associated with a separate identity provider (system that creates, maintains and manages identity information, and provides authentication services). When users attempt to access a remote RADIUS-protected network, they must provide unique user credentials associated with their user identities, stored in a directory database. associated.

After being provided by the user, the login information will be transferred from the client to the RADIUS server via a supplicant (a program that is responsible for fulfilling the login requirements to the wireless network).

Put simply, requests and credentials are sent from the user's device via supplicant to a RADIUS-enabled network device. The RADIUS-enabled network device then forwards the request to the RADIUS server for authentication. Upon receiving the request and user credentials, the RADIUS server will authenticate the user's login credentials to the relevant directory service database.

If the user information matches the information stored in the linked directory database, a valid authentication message will be sent back to the RADIUS client to start connecting to the network. If not, a denial notice will be given.

Limitations of RADIUS

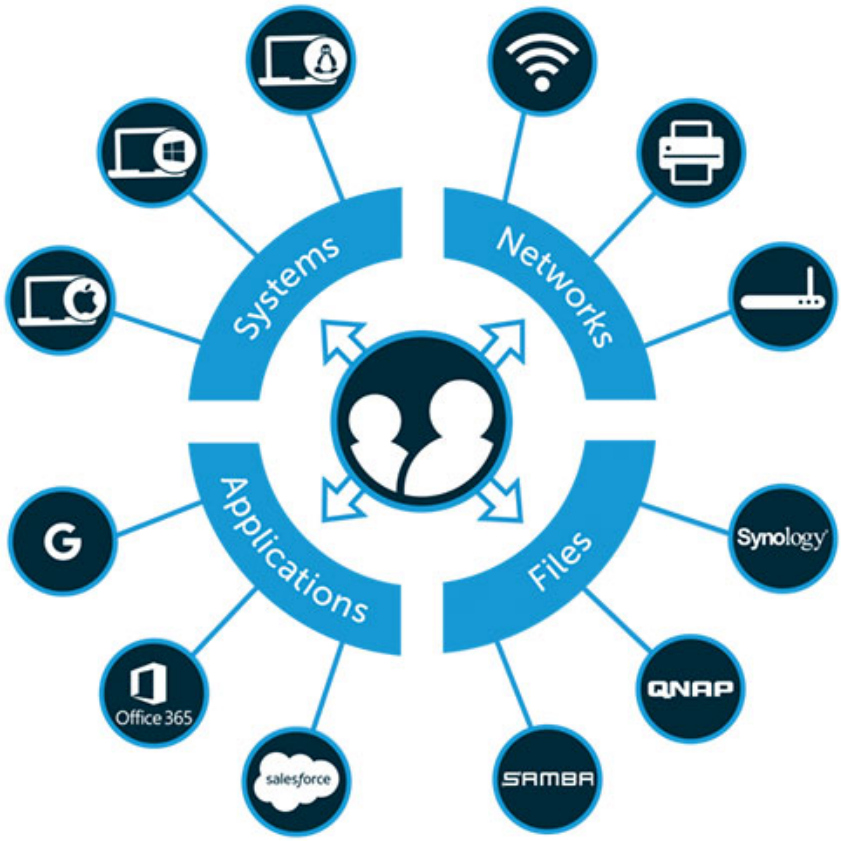
Limitations of RADIUS
The RADIUS protocol has been shown to increase network control and security, but not without certain challenges.

For example, in the past, RADIUS was an on-premise implementation that required efficient on-premises identity management infrastructure to operate (e.g. systems, servers, routers, switches, etc.). .). This setup can be difficult and expensive. Moreover, the on-premises management infrastructure is primarily focused on Microsoft Windows, with Microsoft Active Directory (AD) acting as the main identity provider.

To be fair, AD does not provide its own backend RADIUS function. However, as the modern IT landscape continues to diversify, many IT organizations are turning to AD deployment on-premises, due to its limitations in cross-platform and hybrid-cloud environments.

In fact, many IT organizations are moving their entire on-premises identity management infrastructure to the cloud, with Active Directory alternatives. There are a number of benefits to this approach that increase flexibility and reduce costs, but how IT organizations continue to provide secure RADIUS authentication, without anything being 'on-prem'. ?

RADIUS authentication from the cloud



RADIUS authentication from the cloud
Fortunately, a next-generation identity and access management solution has emerged that can provide RADIUS-as-a-Service, as a cloud-based distribution service.

This solution is called **JumpCloud Directory-as-a-Service** and it not only provides RADIUS authentication from the cloud, but also serves as a comprehensive cloud-based alternative to Active Directory.

This is because JumpCloud is the first cloud-based directory service platform to adopt a vendor-based, protocol-based approach to managing modern IT networks. In doing so, IT organizations can securely manage and connect users to systems, applications, files and networks via RADIUS.

Then, administrators can freely take advantage of the best IT resources for the organization with the peace of mind knowing that they can effectively manage the entire network from the cloud with JumpCloud Directory-as-a. -Service.